COIN in Cyberspace: Focusing Air Force Doctrine Development

Temaat, Martin T.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2006		**00-00-2006 to 00-00-2006**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
COIN in Cyberspace: Focusing Air Force Doctrine Development	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **United States Marine Corps,Command and Staff College, Marine Corps Combat Development Command,Marine Corps University, 2076 South Street,Quantico,VA,22134-5068**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**16**	

No matter what job you’re doing as an Airman, you’re using cyberspace every day. Without it, you couldn’t do your job.

-- Lt Gen Robert Elder, 8 AF Commander

The United States military is heavily reliant on technology to fight and win. Much of this technology relies on cyberspace. The *National Strategy to Secure Cyberspace* and the *National Military Strategy for Cyberspace Operations* were written to address this growing reliance on cyberspace and to guide the armed services in developing their own doctrine. In response, the Air Force changed its mission statement to include flying and fighting in cyberspace and began codifying its cyberwarfare doctrine. This effort is hampered, however, by a limited understanding of cyberspace by rank and file Air Force members. Many believe cyberspace and cyberwarfare are the responsibility of the communications community. If this new doctrine is to be relevant, it must form a clear and direct link[1] between cyberspace and the Air Force's key operational functions.[2] By using existing joint and service doctrine[3] to build upon, the Air Force can create unity of effort among Airmen at all levels, ensure unity of purpose in the prosecution of cyber warfare, and clearly delineate where military responsibility for cyberspace ends and non-military responsibility begins.

Background

Air Force cyberspace doctrine development is based upon DOD's 2006 definition of cyberspace, which states, "cyberspace is a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via

networked systems and associated physical infrastructure."[4] The Air Force refined this further to "cover everything from satellite communication to gamma rays to microwave technologies."[5] The cyberspace domain impacts nearly everything the military services do. This new domain is unlike the land, sea, and air domains, however, because it has no boundaries and cuts across all other domains. These distinctions make it conceptually difficult to understand and operationalize.

Creating Unity of Effort

The Air Force, Army, and Marine Corps have spent considerable time re-evaluating and developing updated counterinsurgency (COIN) doctrine within the last two years.[6] The insights developed from these efforts should be applied to developing cyberspace doctrine because cyberspace and COIN operations have many similarities. For example, tracking down a specific individual to hold responsible for attacks in either environment is nearly impossible. Additionally, attacks are often distributed and numerous groups or factions can attack at the same time. The cyberspace and COIN environments are both constantly changing and adapting as well. Finally, attacks are rarely an end in themselves for attackers. Even when attacks are soundly defeated, the attackers may still accomplish their strategic or operational goals. One of the biggest challenges to developing counterinsurgency doctrine is addressing how

forces trained to produce kinetic effects can fight and win a primarily non-kinetic fight. This is the same major dilemma in cyber warfare.[7]

Numerous differences also exist between cyberspace and COIN operations. For example, most insurgencies are politically motivated, while motivations for cyber attacks can range from criminal intent to national intelligence gathering.[8] The obvious differences[9], however, do diminish the usefulness of COIN doctrine as a framework to focus development efforts. A correct focus will create unity of effort across the Air Force by ensuring personnel understand how their efforts combine to help the Air Force fight and win in cyberspace. This focus will also provide a second-order effect of unifying the public affairs effort surrounding cyberspace, which reinforces a growing culture of "cyberminded" warriors throughout the Air Force.[10] As this new culture develops, the Air Force will begin to benefit from a combined, unified effort of all Airmen to combat and prosecute cyber warfare.

Providing Unity of Purpose

Cyberspace doctrine must also integrate with and supplement other Air Force doctrine. This integration will be difficult because the DOD and Air Force definitions of cyberspace, electronic attack, electronic protection, and computer network operations are all considered part of cyberspace operations.

Current doctrine also places all of these capabilities into the information operations realm as well.[11] This apparent conflict exists because information operations involve protecting and disseminating information, while cyberspace operations are responsible for protecting and managing the systems and transmission paths information traverses. These similarities cause confusion and hinder the average Airman's ability to understand where they fit into the picture or what they are supposed to do to help support the Air Force's efforts.

Integration with current doctrine and a focus on warfighting will ensure effective use of our nascent cyber attack capability. Currently, the Air Force's attack capability is limited by several factors. First, the United States recognizes cyber attacks as acts of war. Consequently, any such acts require the highest levels of political approval before they can be carried out.[12] Further, the Air Force has very few operators that possess the specialized knowledge and skills to perform attacks. Finally, the services do not possess the level of intelligence or the capability to gather the level of intelligence required to execute anything but the most rudimentary attacks.[13] By integrating cyberspace doctrine with special operations and intelligence doctrine, the Air Force will ensure proper levels of training and resources are dedicated to

cyberspace and cyber warfare efforts, which will provide unity of purpose across all functional areas.

As demonstrated, cyberspace doctrine touches nearly every functional area and aspect of air and space doctrine. These interconnections must be documented and addressed throughout the Air Force and across DOD to minimize confusion and maximize effectiveness. If this development effort falls short, the American "Way of War" will find itself increasingly plagued by cyberspace-enabled challenges because of the American tendency to underemphasize alternative belief systems, culture[s], and revolution[s].[14] FM 3-24/MCWP 3-33.5 argues, "the forces that successfully defeat insurgencies are usually those able to overcome their institutional inclination to wage conventional war".[15] Applying this premise to cyberspace doctrine ensures the doctrine will unify not only Air Force efforts, but also help all of DOD's cyber efforts.

Providing Clear Political Boundaries

Enduring principles are what set the military services apart from civilian and other governmental organizations. For example, unity of effort in military operations ensures maximum effects are directed toward the main effort while expending minimum effort on non-essential tasks. Combining unity of effort with the COIN principle of understanding the environment[16]

will help delineate natural boundaries between the myriad of agencies responsible for securing cyberspace.

Understanding the environment in context of this discussion means understanding which agencies have been tasked with securing which pieces of cyberspace. The National Strategy for Homeland Security delineates this as outlined in the table in Appendix 1.[17] This framework allows agencies to benchmark their cyberspace efforts against their operations in other domains to develop effective, workable action plans. Most of these agencies do not coordinate their efforts across the government, however, so projects that benefit one department or agency can conflict with efforts in another.

This confusion is magnified when agencies try to work with the DOD because few truly understand where military responsibility for cyberspace begins and ends. The Air Force should use its cyberspace doctrine to recommend models of how and where these lines of responsibility should be drawn. The service could, for example, base the lines on how the Federal Aviation Administration and military work together to protect and organize the air domain. They could also use how the Navy and Coast Guard combine to protect the nation’s coasts, ports, and waterways as a benchmark for the effort. By recommending lines the Air Force is comfortable with, they can drive the

discussion rather than wait for the fallout when a civilian agency or commission decides for them.

Counterarguments

When developing new doctrine, one of the fundamental decisions to be made is who is going to be responsible for driving doctrine development. Due to the misperception discussed previously, many in the rank and file Air Force would relegate this effort to the communications community. When Air Force senior leadership decided to align the new Cyber Command with Eighth Air Force, they demonstrated their belief that cyberspace effects belong in the operational realm, however. Placing the operational community in charge of cyberspace ensures doctrine integrates with air and space doctrine to produce unity of effort and continuity across all Air Force domains.

Others also argue that COIN doctrine cannot be applied to cyber warfare because COIN operations are primarily about "winning the hearts and minds" of civilians in the operations area. They consider this goal impossible in cyberspace because no equivalent to a civilian population exists. This argument makes COIN operations too simplistic, however. COIN doctrine states that military forces should use whatever combination of efforts (kinetic and non-kinetic) they can to change the local environment on a fundamental level. COIN operations begin by

providing physical security and then systematically working with community leaders to bring about changes that make sense in that local area. This same model can easily be applied to cyberspace. The objective is not to "win the hearts and minds." Rather, it is to combine effects in ways that make sense based on the local environment to achieve the desired end state. Properly integrated cyberspace doctrine will provide the basis for the combination of efforts to happen.

Conclusion

One of the biggest hurdles the Air Force must overcome while developing cyberspace doctrine is the idea that cyberwarfare is about anything other than warfare. Naming a new domain has not changed the fundamental nature of war.[18] New doctrine must augment current doctrine and improve the Air Force's ability to fight in air, space, and cyberspace rather than confuse and diffuse its forces. Refocusing doctrine development on warfighting functions and using established doctrine documents like AFDD 2-3 and FM 3-24/MCWP 3-33.5 will ensure the Air Force has meaningful, relevant cyberspace doctrine that is understandable and usable.

1587 words

Notes

1. David T. Fahrenkrug, “Cyberspace Defined,” *The Wright Stuff*, 17 May 2007, <http://www.au.af.mil/au/aunews/archive/0209/Articles/CyberspaceDefined.html> (12 December 2007), 1.

2. The Air Force has 17 key operational functions: strategic attack, air refueling, counterair, spacelift, counterspace, special operations, counterland, intelligence, countersea, surveillance and reconnaissance, information operations, combat search and rescue, combat support, navigation and positioning, command and control, weather services, and airlift. U.S. Air Force, *Air Force Basic* Doctrine, 2003 (Maxwell AFB, AL: AFDPO), 39.

3. Air Force Doctrine Document (AFDD) 2-3, Irregular Warfare, and Army Field Manual (FM) 3-24/Marine Corps Warfighting Publication (MCWP) 3-33.5, Counterinsurgency can serve as a solid framework to build new cyberspace doctrine upon.

4. U.S. Department of Defense, “Joint Net-Centric Campaign Plan,” *Joint Chiefs of Staff, J6 Command, Control, Communications, and Computer System*, October 2006, <http://www.jcs.mil/j6/c4campaignplan/JNO_Campaign_Plan.pdf> (17 December 2007), 62.

5. J.G. Buzanowski, “Cyberspace expert briefs AFA conference attendees,” Air Force Link, 27 Sep 2007, <http://www.af.mil/news/story_print.asp?id=123069727> (28 Sep 2007), 1.

6. When counterinsurgency oprations are referred to, it is intended to mean both what the Air Force calls “Irregular Warfare” and what the Army and Marine Corps call “Insurgency and Counterinsurgency Operations”. AFDD 2-3, Irregular Warfare was updated in August 2007 and FM 3-24/MCWP 3-33.5 was updated in December 2006.

7. Sebastian M. Convertino II, Lou Anne DeMattei, and Tammy M. Knierim, “Flying and Fighting in Cyberspace,” *Air War College, July 2007,* <http://www.au.af.mil/au/awc/awcgate/maxwell/mp40.pdf> (16 December 2007), pg 14.

8. U.S. Army and U.S. Marine Corps, *Counterinsurgency: FM 3-24/MCWP 3-33.5* (Washington, D.C.: U.S. Army, 2006), 1-22.

9. The list of similarities and differences is not all inclusive. It is meant to be representative and encourage thought.

10. Convertino, DeMattei, and Knierim, iv.

11. Timothy P. Franz, et al., "Defining Information Operations Forces: What Do We Need?," *Air and Space Power Journal Volume XXI*, no. 2 (2007): 56.

12. Convertino, DeMattei, and Knierim, 46

13. Convertino, DeMattei, and Knierim, 44

14. Convertino, DeMattei, and Knierim, 37

15. U.S. Army and U.S. Marine Corps, ix

16. U.S. Army and U.S. Marine Corps, 1-22

17. Convertino, DeMattei, and Knierim, 22

18. Convertino, DeMattei, and Knierim, 65.

Appendix 1

Table 1. Critical Infrastructure Sectors with Lead Agency

Sector	Lead Agency
Agriculture	Department of Agriculture
Food	Meat and poultry: Department of Agriculture
	All other food products: Department of Health & Human Services
Water	Environmental Protection Agency
Public Health	Department of Health & Human Services
Emergency Services	Department of Homeland Security (DHS)
Government	Continuity of government: DHS
	Continuity of operations: all departments and agencies
Defense Industrial Base	DOD
Information and Telecommunications	DHS
Energy	Department of Energy
Transportation	DHS
Banking and Finance	Department of the Treasury
Chemical Industry	Environmental Protection Agency
Postal and Shipping	DHS
National Monuments and Icons	Department of the Interior

Bibliography

Alford, Lionel D., Jr. “Cyber Warfare: A New Doctrine and Taxonomy.” *Software Technology Support Center*. April 2001. <http://www.stsc.hill.af.mil/crosstalk/2001/04/alford.html> (27 October 2007).

Bosker, A.J. “SECAF: Dominance in cyberspace is not optional.” *Air Force Link*. 1 June 2007. <http://www.af.mil/news/story_print.asp?id=123055625> (17 October 2007).

Buzanowski, J.G. “Cyberspace expert briefs AFA conference attendees.” *Air Force Link*. 27 September 2007. <http://www.af.mil/news/story_print.asp?id=123069727> (28 September 2007).

Convertino, Stephen M., II, Lou Anne DeMattei, and Tammy M. Knierim. “Flying and Fighting in Cyberspace.” *Air War College.* July 2007, <http://www.au.af.mil/au/awc/awcgate/maxwell/mp40.pdf> (16 December 2007).

Crane, Conrad C. “Minting COIN.” *Air & Space Power Journal*. December 2007. <http://www.airpower.maxwell.af.mil/airchronicles/apj/apj07/win07/crane.html> (8 December 2007).

Davis, Mary. “AF leader addresses cyberspace defense at conference.” *Air Force Link*. 26 September 2007. <http://www.af.mil/news/story_print.asp?id=123069663> (27 September 2007).

Fahrenkrug, David T. “Cyberspace Defined.” *The Wright Stuff.* 17 May 2007. <http://www.au.af.mil/au/aunews/archive/0209/Articles/CyberspaceDefined.html> (12 December 2007).

Franz, Timothy P., et al. “Defining Information Operations Forces: What Do We Need?.” *Air and Space Power Journal Volume XXI*, no. 2 (2007): 53-63.

Hildreth, Steven A. “CRS Report for Congress: Cyberwarfare.” *Federation of American Scientists*. 19 June 2001.

<http://www.fas.org/sgp/crs/natsec/RS20859.pdf> (18 October 2007).

Howes, Norman R., Michael Mezzino, and John Sarkesain. “On Cyber Warfare Command and Control Systems.” *Defense Technical Information Center*. June 2004. <http://stinet.dtic.mil/cgi-bin/GetTRDoc?AD=ADA465692&Location=U2&doc=GetTRDoc.pdf> (18 October 2007).

Joch, Alan. “Homeland Security’s High-Tech Gamble.” *Federal Computer Week*, 12 November 2007, 17-23.

Levinson, Rob. “What Do We Do Next Time?.” *Air and Space Power Journal*. December 2007. <http://www.airpower.maxwell.af.mil/airchronicles/apj/apj07/win07/levinson.html> (8 Dec 2007).

Lopez, Todd. “Fighting in cyberspace means cyber dominance.” *Air Force Link*. 28 February 2007. <http://www.af.mil/news/story_print?id=123042670> (27 September 2007).

Marquand, Robert and Ben Arnold. “China emerges as leader in cyberwarfare.” *The Christian Science Monitor*. 14 September 2007. <http://www.csmonitor.com/2007/0914/p01s01-woap.htm> (27 October 2007).

Paone, Chuck. “Air Force leaders discuss need to control cyberspace.” *Air Force Link*. 26 September 2007. <http://www.af.mil/news/story_print.asp?id=123069501> (28 September 2007).

Peters, Ralph. “Progress and peril: New counterinsurgency manual cheats on the history exam.” *Armed Force Journal*. (February 2007). <http://www.armedforcesjournal.com/2007/02/2456854> (27 October 2007).

Robinson, Brian. “Gregory Garcia: His First Year as Cybersecurity Czar.” *Federal Computer Week*, 12 November 2007, 26-30.

Rosine, Matthew. “Deciphering Cyberspace: Airmen fending off attacks on a new battlespace.” *Airman Magazine*. Fall 2007.

<http://www.af.mil/news/airman/1107/cyberspace_text.shtml> (6 October 2007).

Rumple, JoAnne. “Commander foresees Air Force mastery of cyberspace.” *Air Force Link*. 29 October 2007. <http://www.af.mil/news/story_print.asp?id=123073727> (29 October 2007).

U.S. Air Force. *Cyber Warfare: Air Force Operational Concept (Draft Version)*. Maxwell AFB, AL: AFDPO, 1 April 2007.

U.S. Air Force. “Doctrine Watch #25: Cyber Space.” *Air Force Doctrine Center*. 11 December 2006. <https://www.doctrine.af.mil/afdcprivateweb/DoctrineWatch/DoctrineWatch.asp?Article=25> (7 December 2007).

U.S. Air Force. “Doctrine Watch #26: The Effects-based Approach to Operations.” *Air Force Doctrine Center*. 31 January 2007. <https://www.doctrine.af.mil/afdcprivateweb/DoctrineWatch/DoctrineWatch.asp?Article=26> (7 December 2007).

U.S. Air Force. *Air Force Doctrine Document 2-3: Irregular Warfare*. Maxwell AFB, AL: AFDPO, 2007.

U.S. Army and U.S. Marine Corps. *Counterinsurgency: FM 3-24/MCWP 3-33.5.* Washington, D.C.: U.S. Army, 2006.

Van der Oord, Larry. “Global Cyberspace Integration Center mission formalized.” *Air Force Link*. 16 October 2007. <http://www.af.mil/news/story_print.asp?id=123071970> (17 October 2007).

Waterman, Shaun. “Analysis: A new USAF cyber-war doctrine.” *United Press International*. 17 October 2007. <http://www.upi.com/International_Security/Emerging_Threats/Analysis/2007/10/17/analysis_a_new_usaf_cyberwar_doctrine/4924/> (27 October 2007).